



Enhanced Dynamic Source Routing (DSR) in MANET

¹Anjesh Kumar, ²Er. Lalit Himral¹Student, ²Sr. Lect.^{1,2} Yamuna Institute of Engineering & Technology, Kurukshetra University
Kurukshetra, Haryana, India

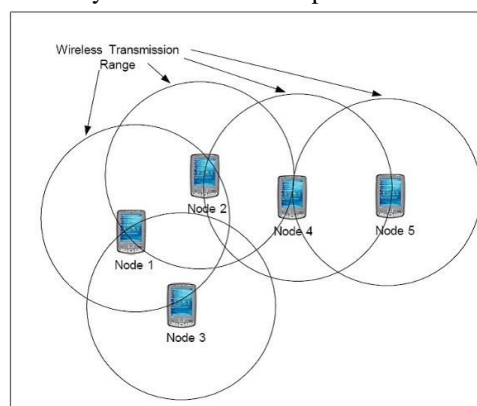
Abstract:-MANET (Mobile Ad-hoc network) is self configuration wireless adhoc network of mobiles node and this type of network is a groups of wireless mobile hosts creating a temporary network without the help of any established (fixed) infrastructure. Every node has a router connected by the wireless connection. Manet (adhoc) may be operate as stand alone network and they may be used to extend the wireless mobile range of a more fixed infrastructure network designs. In Manet every nodes move freely and independently so this type of topology is highly dynamic compare to fixed network. Because of limited transmission power of active nodes multiple hops may be required to transfer data from one host to another host. Main challenges in mobile adhoc is bandwidth limitations, battery problems, Routing Overheads & Hidden terminals, dynamic topologies and Packet losses due to transmission errors. DSR is important protocol used in MANET network. This paper proposes a new reputation scheme on DSR protocol based and through simulation results, it is proved that proposed method performs well compared to normal DSR. By using new scheme DSR reputation based protocol, PDR is above 99% which is very high compare to normal DSR.

Keywords: Reputation based DSR, DSR, Ad-hoc network, Manet network, Security, Energy efficiency, wireless networking problems.

I. INTRODUCTION

Manet ad-hoc network is an independent system of mobile hosts connected by wireless links. No fixed setup such as base station and routers. If two hosts are not within the wireless range then all message communication between them must pass through one or more middle hosts that double as routers. The hosts are independently move randomly in this type of network and thus making the network topology dynamically.

Almost all mobile devices are supported by battery powers, so the energy efficient issue is one of the most important design issues in MANET. Many routing protocols have been proposed as the origin of Manet. Dynamic Source Routing is popular routing protocol which is based on source routing. In this type of networks, different nodes move freely and independently, so this topology is highly dynamic. The Mobile Adhoc network is a group of wireless mobile hosts founding a temporary network without the help of any established infrastructure/centralized direction. Under these circumstances, routing is much more complex than static networks. Adhoc network may be used in area where infrastructures for mobile communication are not available due to high deployment costs or disaster destruction of infrastructure. Due to lack of infrastructure and the limited transmission range of a node in a mobile ad hoc network, a node have to rely on neighbors nodes to route a packet to destination nodes. In this types of manet network, working are based on the node cooperation. Routing protocols for mobile ad-hoc networks, such as the DSR (Dynamic Source Routing) and the Ad-hoc On Demand Distance Vector Routing Protocol (AODV) are based on the assumption that all nodes will co-operate and without node co-operation, in a wireless adhoc network, no route can be established and no packet can be forwarded in this type of network. The Dynamic Source Routing protocol (DSR) is a simple & well organized routing protocol designed specifically for use in multi-hop wireless ad-hoc networks of mobile nodes.



Manet Adhoc (Figure-i)

In Manet network to send a packet to another host sender node create a source route in the packet header and giving the address of each host in the network through the packet should be forwarded in order to reach the target host. Sender side node then transmits these packets over its wireless network interface to the first stage identified in the source route. when host receives a packet and if this host is not the final destination of the packet then it transmits the packet to the next stage identified in the source route in the packet header. when packet reach it's final destination then the packet is delivered to the network layer software on that host. Every host participating in the ad-hoc network maintains a route history in which it store source routes. When one host send a packet to another host then the sender checks its route history for a source route to the destinations and if a route is found then sender uses this route to transmit the packets and if no route is found then the sender may try to discover using the route discovery protocol.

II. ROUTE DISCOVERY

Route discovery are used when source node desires a route to a destination node. Source node found its route cache to determine if it already contains a route to the destination. If the source node found valid route to the destinations and it use this route to send its data packets. If a node have a valid route to the destination then it recruit the route discovery process by broadcasting a R message and Route request (RR) message have the address of the source and the destination and a unique identification number.

Middle node that receives a route request message searches its route cache for a route to the destination. If no route is found then it appends its address to the route record of the message and forwards the same message to its neighbors. The message range through the network until it reaches either the destination or an intermediate node with a route to the destinations. RR (Route reply) message having the proper hop sequence for reaching the destination is made and unicast back to the source node.

III. ROUTE MAINTENANCE

Route Maintenance is used to handle route breakage. In case, a node come crossways a final transmission problem at its data link layer then it removes the route from its route history and generates a route error message. Route error message is sent to every node and it has sent a packet routed over broken link. Whenever a node receive a route error message and it delete the hop in error from its route caches.

Acknowledgment messages are used to verify the correct operation of the route linkage. In wireless networks for e.g. IEEE802.11 immediate provides acknowledgments. In case a built in acknowledgment mechanism is not available then the node transmitting the message can explicitly request a DSR-specific software acknowledgment to be returned by the next node along the route.

IV. DYNAMIC SOURCE ROUTING (DSR)

Dynamic source routing protocol (DSR) is an on-demand protocol designed to control the bandwidth expended by control packets in ad hoc wireless networks by removing the broken table update messages required in the table driven method and main difference between this and the other on-demand routing protocols is that it is beaconless and hence does not require interrupted hello packet transmissions which are used by a node to inform its neighbors of its existence. Main approach of this protocol during the route construction phase is to establish a route by submerging RouteRequest packets in the network. Destination node on receiving a (RR) router request packet and responds by sending a route reply packet back to the source which carries the route traversed by the RouteRequest packet received.

In designing of DSR, we sought to create a routing protocol that had very low overhead yet was able to react very quickly to changes in the network. The DSR protocol provides reactive services in order to help ensure successful delivery of data packets inspite of node movement or other changes in network conditions.

DSR protocol is a group of two main mechanism which work together to allow the discovery and maintenance of source routes in the adhoc network.

Route Discovery is the mechanism by which a node S wishing to send a packet to destination node E obtains source route to E. Route Discovery is used only when S attempts to send a packet to E and does not already know a route to E.

Route Maintenance is the mechanism by which node S is able to detect when using a source route to E and if network topology has changed such that it can no longer use its route to E because a link along the route no longer works.

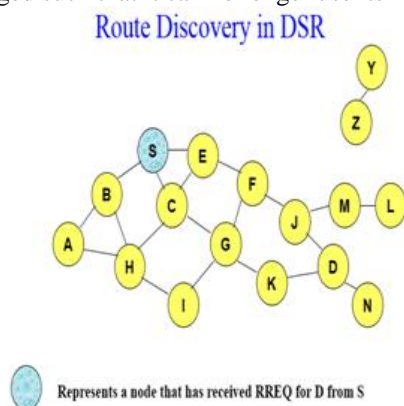


Figure-ii

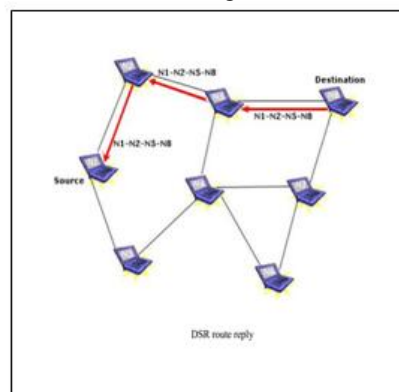


Figure-iii

As & when Route Maintenance show a source route is broken and S may attempt to use any other route it happens to know to E then it can raise route discovery again to find a new route for subsequent packets to E. route and maintenance required for this route is used only when S is actually sending packets to E. Different type operations of Route Discovery and Route Maintenance in DSR are designed to allow unidirectional links and asymmetric routes to be supported.

V. PROPOSED WORK

PROPOSED WORK

PROTOCOL ARCHITECTURE:-

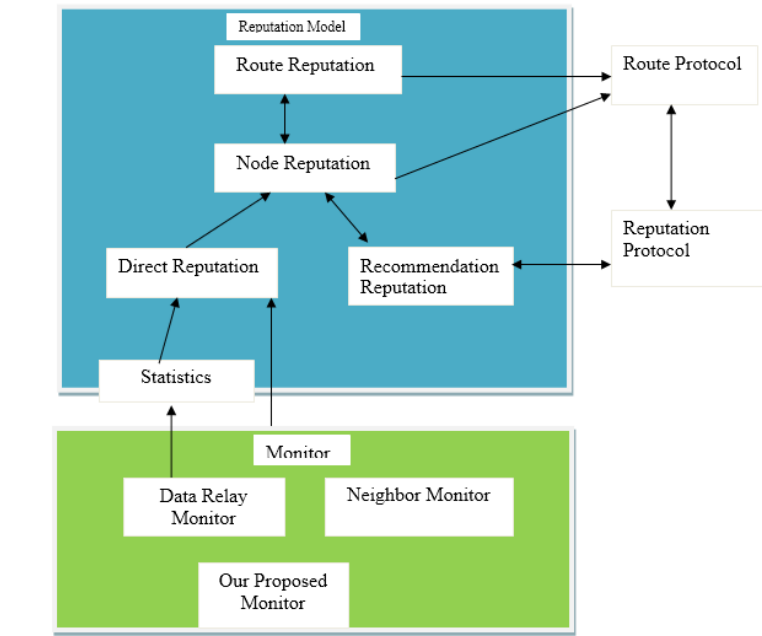


Figure-iv

MONITOR: This part includes three modules: neighbor monitor, data relay monitor, and CoF monitor. Neighbor monitor works with MAC layer. It is used to monitor neighbors in its radio range and maintain neighbor list. Data relay monitor is placed in the network layer. It requires MAC layer working in promiscuous mode, so that it could check whether the next hop had transmitted its packets. CoF would collect information about capability of forwarding from physical layer and MAC layer, and it includes node's bandwidth, interface state, mobility status, and power.

STATISTICS: This module is responsible for providing statistics data about neighbors' history behavior. These data include the number of requested and forwarded protocol messages, and data packets.

REPUTATION model: This is the core module of. It is used to evaluate node's reputation and integrate route reputation relying on the data from MONITOR and STATISTICS.

REPUTATION PROTOCOL: This part defines reputation discovery in the MANET.

ROUTING PROTOCOL: It is an extension of DSR by reputation model.

In the scenario some of mobile nodes communicate with another nodes located on the simulation area. The traffic will be a TCP source.

Simulation Parameters & Performance Metrics

The packet delivery ratio is defined as the number of received data packets divided by the number of generated data packets. Data drop, which is caused, by dropping data packets that is forwarded to it and it drop without transmitting and abnormally under pause of time.

Throughput it is the ratio of the number of packet delivered to the number of forwarded.

Routing overhead that is occurred due to the Link creation and the Link breakage.

Table-1

Parameter	Value
Number of Nodes	50
Number of Traffic Sources	1
Type of Traffic	FTP
Packet Size	512 bytes
Topology Area	1200m X 1200m
Mobility Patterns	Random waypoint
Routing Protoco	DSR

VI. RESULTS AND DISCUSSION

We have simulated the proposed approach using NS 2.34. Network simulator is event oriented simulation tolls which is used for wired and wireless networks. We have taken network of 50 nodes. Rest simulations parameters are as per parameters list.

In below mentioned table, we have simulate the result for the simulation time of 20,25,30 and 35. As mentioned in Table-2, the packet drop for different simulation time is constant i.e. 20 and PDR is greater than 99%. In normal DSR, the packet drop is high i.e 57.6807,65.151,69.5503,76.5594 (as per table -4) compare to reputation based DSR protocol.

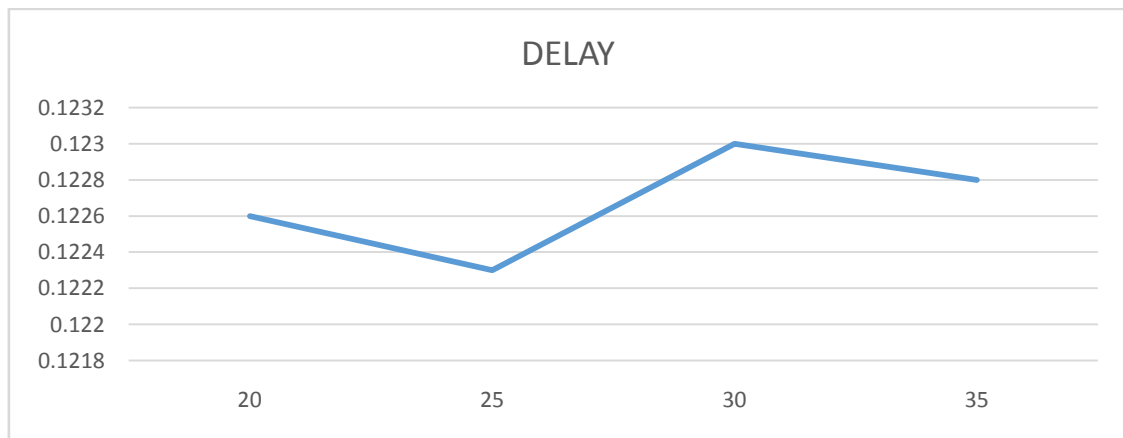
Table-2

DSR WITH REPUTATION						
Simulation time	Packet received	Packet Sent	Drop	Delay	Throughtput	PDR
20	3066	3086	20	0.1226	613332	99.35191
25	3880	3900	20	0.1223	621022	99.48718
30	4676	4696	20	0.123	623615	99.57411
35	5496	5516	20	0.1228	628218	99.63742

Refer to table -3, we have shown the DSR with reputation and we have also shown the same through hart also i.e. Figure-V, VI, VII

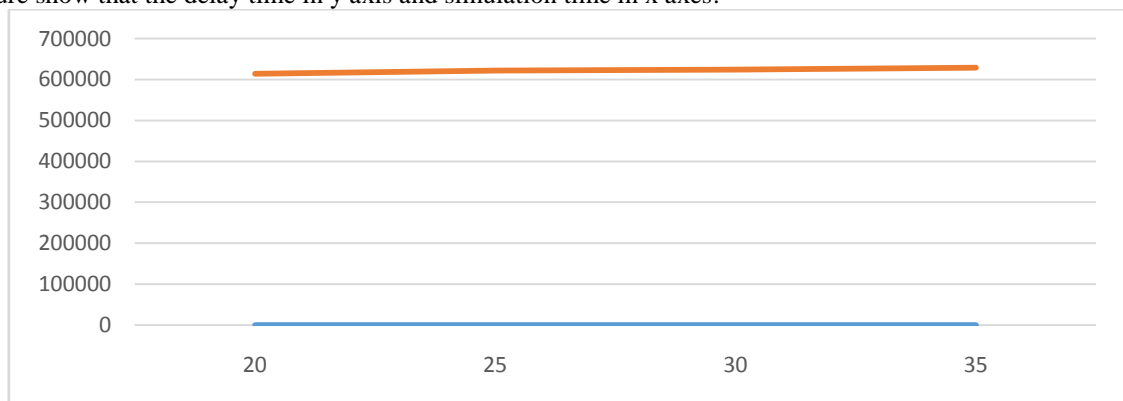
Table -3

Simulation time	Delay	Throughtput	PDR
20	0.1226	613332	99.35191
25	0.1223	621022	99.48718
30	0.123	623615	99.57411
35	0.1228	628218	99.63742



Simulation Time
Figure -v

The figure show that the delay time in y axis and simulation time in x axes.



Simulation Time
Figure-vi

In figure-vi, we have shown the throughput of different simulation times.

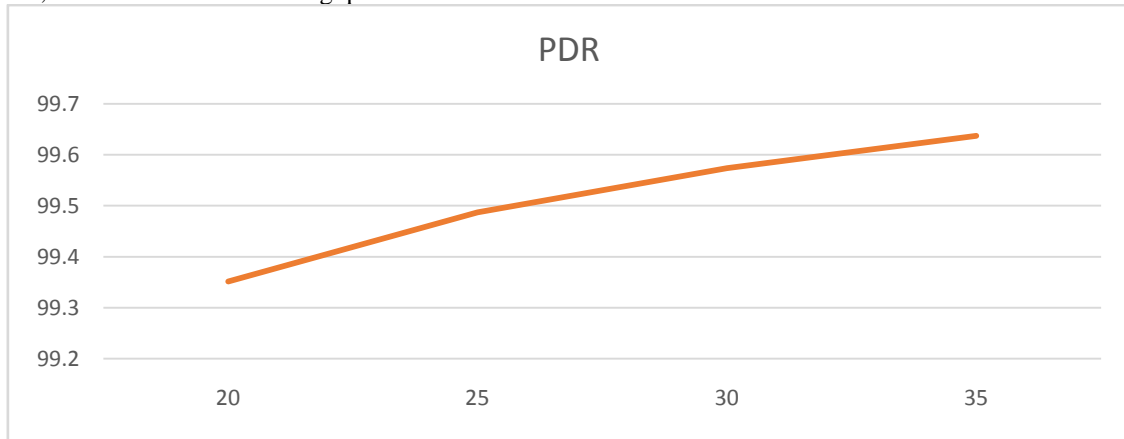


Figure -vii

In figure- vii, PDR in different simulation time has shown, the PDR ratio is greater than 99% and increase efficiency. Refer to the table-4, if we use normal DSR(Dynamic source routing) then packet delay time are greater than 56%, result efficiency down of network and delay in network.

Table-4

NORMAL DSR PACKET DROP	
Simulation Time	DSR(packet drop)
20	57.6807
25	65.151
30	69.5503
35	76.5594

Comparison in Normal DSR and DSR with reputation based

Refer to table-5, in which packet drop comparison has shown, comparatively DSR reputation packet drop are more efficient and increase the efficiency of network.

Table-5

Simulation Time	DSR packet drop	DSR -Reputation packet drop
20	57.6807	20
25	65.151	20
30	69.5503	20
35	76.5594	20

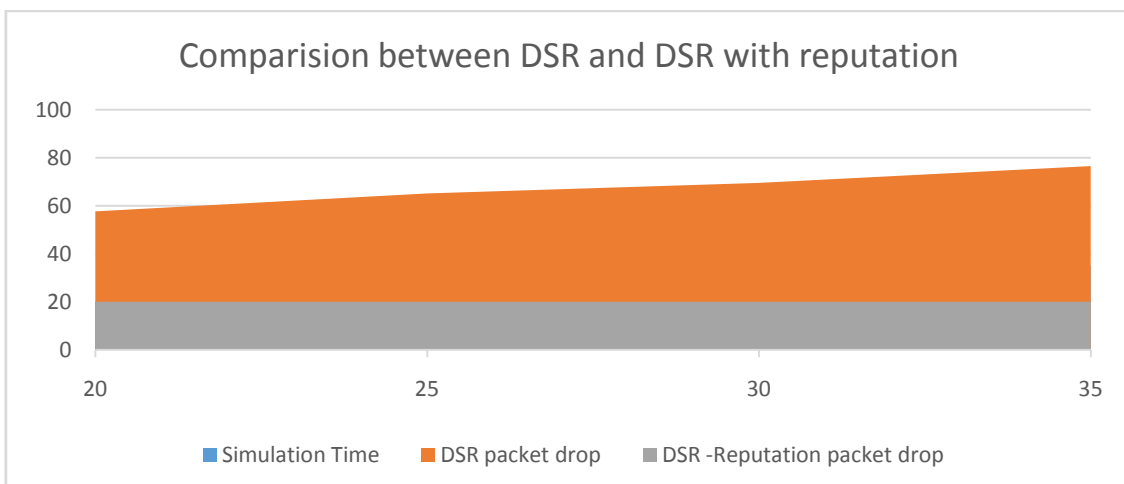


Figure-viii

VII. CONCLUSION

In this research paper, we have shown a DSR reputation scheme for adhoc network to increase the route reliability between the nodes available in network. Our motive and approach to increase the efficiency of network is to calculate the reput value of nodes by using cache memory. Also we check the behavior of node, if route is not perfect or in looping then we use different route which takes less time. In this research, secure and safe routing has been selected for sender and receiver communications so that packet loss can be minimized and malicious and selfish nodes are ignored in DSR reputation. By using the DSR with reputation, we have found that we have increase the performance of network and reduce the packet loss.

REFERENCES

- [1] Bowman, T.H. Lacey et al., "RIPsec Using reputation-based multilayer security to protect MANETs", *computers & security* 31 (2012) 122 -136
- [2] Lakshmi P.S., Pasha Sajid and Ramana M.V.3 "Security and Energy efficiency in Ad Hoc Networks" *Research Journal of Computer and Information Technology Sciences* Vol. 1(1), 14-17, February (2013)
- [3] Azzedine Boukerche et al., "Routing protocols in ad hoc networks: A survey", *Computer Networks* 55 (2011) 3032–3080.
- [4] Md Shahid Akhter¹, Vijay Prakash Singh² "MODIFIED POWER SAVING DSR PROTOCOL FOR MANET" Vol. 2, Issue 6, June 2013.
- [5] Kavita Sharma "Energy Efficient Power Aware Multipath Dynamic Source Routing" *International Journal of Computer Science and Network Security*, VOL.14 No.8, August 2014.
- [6] J.-E. Garcia, A. Kallel, K. Kyamakya, K. Jobmann, "DSR-based Energy-efficient Routing"
- [7] Palak¹, Nasib Singh Gill² "Power Saving Intelligent Dynamic Source Routing (IDSR) in MANET" *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 3, Issue 7, July 2014.
- [8] Jean-Marc Robert, Hadi Otrok, Abdelkarim Chriqi, "RBC-OLSR: Reputation-based clustering OLSR protocol for wireless ad hoc networks", *Computer Communications*, 35 (2012) 487-499
- [9] Abdelwadood Mesleh "AODV and DSR energy-aware routing algorithms" *International Journal of Computer Science Issues*, Vol. 9, Issue 6, No 1, November 2012 ISSN (Online): 1694-0814.
- [10] FeiWang, FurongWang, Benxiong Huang, and Laurence T. Yang" A Reputation-Based Secure Route Protocol in MANET" *EURASIP Journal on Wireless Communications and Networking* Volume 2010, Article ID 258935, 10 pages doi:10.1155/2010/258935
- [11] Mohammed Hawa, Sinan Taifour et al., "A dynamic cross-layer routing protocol for Mobile Ad hoc Networks", *Int. J. Electron. Communication. (AEÜ)* 66 (2012) 996– 1005.
- [12] Gurwinder Singh, Chakshu Goel , Gurjeevan Singh "An Enhancement over Dynamic Source Routing Protocol in Multi-hop Wireless Ad-hoc Network"
- [13] Sangheetaa Sukumran "Reputation based Dynamic Source Routing Protocol for MANET" *International Journal of Computer Applications* (0975 – 888) Volume 47– No.4, June 2012.
- [14] D.B. Johnson, D.A. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*, *Mobile Computing*, 1996.
- [15] Dr.A.Rajaram "Power Aware Routing for MANET Using Ondemand Multipath Routing Protocol" *IJCSI International Journal of Computer Science Issues*, Vol. 8, Issue 4, No 2, July 2011 ISSN (Online): 1694-0814
- [16] Rachit Jain "Performance Comparison of AODV & DSR on the basis of Path Loss Propagation Models" .
- [17] Reputed-DSR: An Enhancement over Dynamic Source Routing Protocol in Multi-hop Wireless Ad-hoc Network ISSN: 2319-1120 /IJAEST/V2N1:01-11 ©IJAEST
- [18] David B. Johnson "Dynamic Source Routing in Ad Hoc Wireless Networks" *Computer Science Department Carnegie Mellon University 5000 Forbes Avenue Pittsburgh, PA 15213-3891*
- [19] Gurwinder Singh "Reputed-DSR: An Enhancement over Dynamic Source Routing Protocol in Multi-hop Wireless Ad-hoc Network" *International Journal of Advances in Engineering Science and Technology*
- [20] S. Mohapatra, P.Kanungo, "Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator" *Procedia Engineering* 30 (2012) 69 – 76
- [21] Jihye Kim " Secure route discovery for dynamic source routing in MANETs". *Ad Hoc Networks* Volume 7, Issue 6, August 2009, Pages 1097–1109
- [22] Asad Amir Pirzada et al., "Incorporating trust and reputation in the DSR protocol for dependable routing", *Computer Communications* 29 (2006) 2806–2821
- [23] Boon-Chong Seet, Bu-Sung Lee and Chiew-Tong Lau "Route discovery optimization for dynamic source routing in mobile ad hoc networks" *Route discovery optimization for dynamic source routing in mobile ad hoc networks* Boon-Chong Seet, Bu-Sung Lee and Chiew-Tong Lau" Singapore 639798.
- [24] Eiman Alotaibi, Biswanath Mukherjee, "A survey on routing algorithms for wireless Ad-Hoc and mesh networks", *Computer Networks* 56 (2012) 940–965.
- [25] PATROKLOS G et al., "Secure Routing for Mobile Ad-hoc Networks", *IEEE Communication and Surveys*, Third Quarter 2005, vol. 7, no.3
- [26] Yacine Rebahi, Vicente .E Mujica-V, Cyprien Simons and Dorgham Sisalem, "SAFE: Securing pAcket Forwarding in ad hoc networks", *Fraunhofer Fokus, Kaiserin Augusta Allee 31, 10589 Berlin, Germany*

- [27] Lalit Himral “Preventing AODV Routing Protocol from Black Hole Attack”, International Journal of Engineering Science and Technology (IJEST)
- [28] www.sciencedirect.com
- [29] www.portal.acm.com
- [30] <http://www.isi.edu/nsnam/dist/nsallinone-2.28.tar.gz>
- [31] <http://www.isi.edu/nsnam/ns/ns-problems.html>
- [32] Ns2 - www.isi.edu/nsnam/ns/ns-tutorial/tutorial-02